UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA, : No. 14 Cr. 68

- against - :

ROSS WILLIAM ULBRICHT, :

Defendant-Petitioner. :

----------X

MEMORANDUM OF LAW IN SUPPORT OF MOTION REQUESTING DISCOVERY PURSUANT TO 28 U.S.C. § 2255

Paul Grant
Law Office of Paul Grant
19501 E. Mainstreet, Suite 200
Parker, CO 80134
Tel.: 303-909-6133
Email: paul_pglaw@yahoo.com
Counsel for Mr. Ulbricht

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

INTRODUCTION

Mr. Ulbricht was tried in this court in a 13 day jury trial and on February 4, 2015, his jury brought back guilty verdicts on all charges in the indictment. Mr. Ulbricht was sentenced on May 28, 2015, to serve two concurrent life sentences, plus 40 years. Mr. Ulbricht's direct appeal was denied on May 31, 2017, and on June 28, 2018, the Supreme Court denied his Petition for Writ of Certiorari. Docket No. 17-950. Mr. Ulbricht is currently serving his sentence in the United States Penitentiary in Tucson, Arizona.

Mr. Ulbricht is now developing his motion pursuant to 28 U.S.C. § 2255 (his "habeas petition"), to vacate, set aside or correct his sentence, because: his sentence was imposed in violation of the Constitution or laws of the United States; or the court was without jurisdiction to impose such sentence; or the sentence was in excess of the maximum authorized by law; or the sentence is otherwise subject to collateral attack. Mr. Ulbricht's habeas petition is due on or before 1 year from the date on which his judgment of conviction became final, thus, it is due on June 28, 2019. 28 U.S.C. § 2255 (f)(1).

Mr. Ulbricht is now requesting leave from the court, and authorization, to discover the contents of three sealed magistrate files, files which should, as required by statute, contain evidence which either corroborates or contradicts the

statements made under oath by law enforcement in their search warrant applications when they sought, and obtained, search warrants authorizing the seizure and search of Mr. Ulbricht's laptop computer, and authorizing the search of his residence. Those files may also show whether the FBI's data collections efforts exceeded the authorization provided by the pen-trap orders.

STATEMENT OF FACTS

Post-conviction counsel for Mr. Ulbricht requested discovery from the United States Attorney's Office ("USAO") relating to data collected pursuant to several pen-trap orders,[1] all dated in September 2013. Declaration of Paul Grant, ¶ 3. The USAO advised (in November 2017) that they were searching for those records in FBI files. Id. ¶ 4. The USAO advised that they found it difficult to locate the files, given that the lead agents involved in the investigation no longer worked for the FBI, but the USAO advised post-conviction counsel on Friday, February 2, 2018, that they had located some pertinent files, files containing pen register and trap and trace data collection ("PRTT files"), and that they would be sending that data to undersigned counsel on a disk. Id. ¶ 4. Undersigned counsel also requested those files and FBI surveillance files through a FOIA request sent to the FBI, but the FBI has recently said that some of the records being sought are in

[1] Orders which in this case authorized the collection of pen register or trap and trace data from computer networks supposedly used by Ulbricht.

the control of the Executive Office for United States Attorneys. Id. ¶ 6. That FOIA request has not produced any records. Id.

The requested PRTT files are material to determining whether the government complied with the law in collecting PRTT data, and whether the FBI collected the data they claim (in the search warrant applications and under oath in opposing Mr. Ulbricht's Motion to Suppress) they collected, and whether the search warrant affidavits contained material falsehoods. The affidavits submitted in support of the laptop search warrant and the residence search warrant, both relied upon evidence allegedly collected pursuant to the pen-trap orders. No such PRTT data (as claimed in the laptop and residence search warrant applications) was ever produced in discovery, despite defense requests - both before trial and post-conviction.

Results from only one pen-trap data collection effort were provided to the defense prior to trial, despite the fact that the government apparently conducted pen-trap data collection pursuant to five separate pen-trap orders. Grant Decl. ¶ 8. Post-conviction counsel has requested from the USAO the data collected pursuant to four other pen-trap orders, the orders identified by magistrate case numbers as 13 MAG 2228, a Sealed Order for the Secret Service directed to Comcast, 13 MAG 2258 (the 9.19.13 wireless router pen for FBI), 13 MAG 2274

((9.20.13.Router Pen for FBI), and 13 MAG 2275 (9.20.13.MAC Address Pen for FBI). Grant Decl. ¶ 3.

Mr. Ulbricht has recently obtained expert assistance in examining the one set of PRTT data produced by the government pre-trial, and in examining the additional PRTT data provided by the government in February 2018. Grant Decl. ¶ 9.

Defendant Ulbricht did make a written discovery request to the government before trial for *any and all data obtained from pen registers judicially authorized in this case*. Doc (Docket #) 70-3, Par. 13, p. 3, 9/17/2014 letter from Joshua Dratel to AUSAs Serrin Turner and Timothy T. Howard. That request was for data material to preparation of the defense. In response to Ulbricht's request for discovery of *any and all data obtained from pen registers judicially authorized in this case*, the government responded (rather ambiguously):

"The Government has provided all available pen register data used to detect Ulbricht's email and Internet activity in September 2013, as well as pen register data received from Icelandic law enforcement authorities concerning the SR Server and the server described in the Tarbell Declaration as Server-1. To the extent any other pen register information was obtained in the course of the investigation, the Government objects to this request on the ground that such information is not

material to the defense or otherwise required to be produced under Rule 16." See Doc 70-4 at p. 5, 9/23/2014 letter from AUSA Serrin Turner to Joshua Dratel.

The government's response was carefully worded in a manner that avoided stating whether the pen register data [supposedly] used to detect Ulbricht's internet activity was available, or not, and whether it was or was not provided, and, at the same time, the government said that if pen register data was not available, then it was not material and they were not required to produce it.

It was not clear from that response whether the government was saying that the pen register data used to detect Ulbricht's internet activity in September 2013 was provided, or whether it was not available, or whether the government had not provided it because the government decided it was not material to the defense or otherwise required to be produced under Rule 16. What is clear from this crafty response, is that the government had covered all of its bases in that ambiguous but carefully worded statement, and that it had denied any obligation to provide any data at all.

Defense counsel at trial ("trial counsel") may not have realized that he never received the PRTT data ("pen register data") that the search warrant applications referenced, and he may never have realized what PRTT data he had received, and

what data he had not received. Grant Decl. ¶ 10. It does not appear that trial counsel ever examined any PRTT data. Id.

Post-conviction counsel has had an expert examine the PRTT data produced in discovery prior to trial, and that expert has determined that the data produced appears to have been collected by internet service provider Comcast, and not by the FBI. The government only produced to the defense the data collected pursuant to one pen-trap order, data in a file that the government called Ulbricht Home Comcast 67.169.90.28. Grant Decl. ¶ 8. The pen-trap order that led to that data collection appears to have been an order directing Comcast cooperation and authorized by the magistrate on September 17, 2013. Doc. 47, Dratel Decl. ¶ 3(d). That order authorized the use of pen register devices for the identification of source and destination IP addresses communicating with the Comcast account, and did not authorize the collection of MAC addresses (used to identify devices on the local network) and did not authorize collection of routing data involving any data transmitted from or to any device identified by a MAC address, and that order did not seek data collection to monitor internet activity from Mr. Ulbricht's computer. *Id.*

Four other pen-trap orders were obtained in September 2013 for data collection regarding network activity at Ulbricht's residence, but no data was ever

produced in discovery for any of those other four orders, yet the laptop search warrant cites the results from two of those orders, orders which did authorize the collection of MAC addresses, and which did authorize collection of data transmitted to or from devices associated with certain MAC addresses. Doc. 57, Tarbell Decl. ¶ 19. No PRTT data resulting from either of those two pen-trap orders was ever produced in discovery, despite the fact Tarbell stated in his declaration that the pen registers were used to collect the MAC addresses of the devices connecting to the router in Ulbricht's residence. Id. Tarbell also offered his explanation, under oath, that "A media access control address, or "MAC address," is a unique identifier embedded in the hardware of devices with a network interface, which can be used to identify the device on any network the device connects to." Doc. 57, Tarbell Decl. fn 11.

Mr. Sayler disagrees with Tarbell's statement that a MAC address is unique, and he disagrees with the value of a MAC address for identifying a device on a network. Sayler Decl. 15. Sayler stated that he knows from his own study and work that changing a MAC address is a trivial operation on most systems. He states that he published an article on that subject in 2011. Id.

Mr. Sayler also said he understood that when Ulbricht's laptop was seized, it was running Ubuntu Linux, and that "on Ubuntu Linux it would have been a trivial

step to change the MAC address of the laptop. Ulbricht could have collected other MAC addresses on any network he used, and then substituted other MAC addresses for his own. Similarly, other users on networks used by Ulbricht could have collected the MAC address from Ulbricht's computer, and used his MAC address as their own. . . The fact that MAC addresses can be easily changed is widely known." Sayler Decl. ¶ 16.

The government stated that the pen registers were used to establish when Ulbricht logged onto and off of the internet, in support of their argument that the search warrant applications to search for information to allow comparison with online activity were reasonable requests seeking relevant and permissible information, not tracking information, referencing Doc. 57, Tarbell Decl. ¶ 21. See Doc. 56, Memorandum of Law in Opposition to Defendant's Motion to Suppress, at p. 29 of 58.

Mr. Sayler stated that he has not seen any data that would allow the FBI to claim that it had collected data that showed any device communicated to or from Ulbricht's computer. Sayler Decl. ¶ 22.

There is new information which has recently (since Ulbricht's trial) become available that indicates that the government did use electronic surveillance as part of its pen register data collection, to track and determine Ulbricht's precise location

in his residence, and to determine when he "logged in" and out on his laptop, while Ulbricht was in his residence. This information is provided in the pages of the book titled "American Kingpin," a book published in May 2017, more than two years after the trial was concluded.

According to the author, Nick Bilton, his accounts are based, in part, on more than 250 hours spent with federal agents involved in the investigation,[2] including FBI special agents he identifies [Christopher Tarbell and Thomas Kiernan], and including Homeland Security Investigations special agent Jared Der-Yeghiayan. Bilton's account of FBI surveillance correctly places Tarbell, Der-Yeghiayan, and Kiernan on site outside Ulbricht's residence, a short time before Ulbricht's arrest. He describes the actions and observations of these agents. His account is credible. Grant Decl. ¶ 11. Bilton describes the FBI surveillance of Ulbricht in his residence:

"Jared [Der-Yeghiayan], Thom [Thomas Kiernan], and Brophy stood in front of the café near Ross' house, listening to Tarbell . . . They knew that Ross was at home because the FBI had an undercover SUV circling his block and monitoring the Wi-Fi traffic (this is pen register and trap and trace activity). The system they were using (which should be described in the magistrates' files) would

[2] "American Kingpin" at 324.

check the signal strength of the Wi-Fi on his computer and then, by triangulating that data from three different points they had captured as they drove around the block, they were able to figure out Ross's exact location, which at this very moment was his bedroom, on the third floor of his Monterey Boulevard apartment." "American Kingpin" (hardcover edition) at 283.

Mr. Ulbricht has obtained expert assistance to examine the one set of PRTT data (in pcap format) produced by the government pre-trial, and to examine the additional PRTT data provided to post-conviction counsel by the government in February 2017, data that was provided in csv format. Grant Decl. ¶ 9. That expert has also commented on various statements made by Christopher Tarbell in his Declaration (Doc. 57) [redacted], and he has examined the search warrant materials the government used to obtain a search warrant authorizing the government to seize and search Mr. Ulbricht's laptop computer. *Id.*

Mr. Ulbricht's expert, Andrew Sayler, is an expert in the field of computer and information security and computer systems, and holds a PhD and MS in Computer Science. Sayler Decl. ¶ 1. Mr. Sayler examined the PRTT data (in the form of pcap files) that was provided to him by undersigned counsel, the same PRTT data that was provided to Ulbricht in discovery. Sayler Decl. ¶ 3.

Mr. Sayler determined that the pcap files appeared to contain wide area network (WAN) traffic involving communications between a cable modem and other servers on the internet. Sayler Decl. ¶ 4. All of the files he examined showed bidirectional traffic, always involving a Comcast IP Address as one end of each exchange. Id. This type of traffic could be collected by Comcast outside of the home where the router was located, without needing to break any WiFi encryption or otherwise monitor the local-area network (LAN) in the home. Id.

None of the pcap files examined appeared to contain any local-area network (LAN) or WiFi traffic internal to the house where the modem was located. Sayler Decl. ¶ 5. None of the pcap files appeared to identify any of the MAC addresses internal to the home network or WiFi. Id. at ¶ 6. Those files showed only the external MAC address of the modem itself, plus MAC addresses of other Internet systems, most likely routers on the Comcast network. Id. All of the internal MAC addresses (for devices using the home network) would have been stripped by the home's router from the network traffic examined, before the traffic entered Comcast's network, where it appears that the data was collected. Id.

According to Mr. Sayler, there is no way to determine from the network traffic (PRTT data) provided in discovery, who within the house originated that network traffic, and there is no way to determine whether that traffic involved a

single individual or multiple individuals, absent additional information. Sayler Decl. ¶ 7.

Mr. Sayler stated that he examined two court orders authorizing PRTT data collection by Comcast, and that the pcap files he was provided and examined, appear to correspond with what was authorized for collection in the court order [redacted] Sayler Decl. ¶ 8.

Mr. Sayler also examined additional PRTT data provided to him by undersigned counsel, data in a csv (comma-separated value) format. Sayler Decl. at ¶ 9. That data and the data provided to him as pcap files, appears to have been all of the PRTT data that was ever provided to Mr. Ulbricht by the government. Grant Decl. ¶ 12. Mr. Sayler stated that the csv files appear to contain a processed version of the same pcap data he previously examined. Sayler Decl. ¶ 9.

Mr. Sayler was provided with search warrant materials relating to the laptop search warrant obtained by the government. Sayler Decl. at ¶ 10. He reviewed those materials, including the affidavit provided [redacted] in support of the search warrant application. Id. [redacted]

[redacted] Mr. Sayler was tasked with examining the affiant's sworn statements, to identify possible examples of inaccuracy or factual incorrectness, where possible.

Mr. Sayler describes the affiant as having stated that [redacted]

Mr. Sayler reviewed two pen register applications requested on 9/20/2013, where orders was obtained and identified as [redacted]. Id., at ¶ 12. The first pen-trap order authorized the collection of MAC addresses associated with communications sent to or from the home router, and the second order authorized the government to capture communications involving any computer associated with any of several different MAC addresses. Sayler Decl. ¶ 12; Doc. 47 ¶¶ 3(g), 3(h).

None of the data examined by Mr. Sayler showed any of the [redacted], nor did it show the identification of any MAC address of any devices on the LAN network. Sayler Decl. at ¶ 13. Mr. Sayler saw no data which showed that any MAC addresses were collected by the government, [redacted]

[redacted]. Id. Mr. Sayler stated that the data he was provided does not show how the FBI obtained the MAC address of Mr. Ulbricht's computer. Id. FBI special agent Christopher Tarbell did state, under oath, that the FBI collected MAC addresses of the devices using the router at Ulbricht's residence. Doc. 57, Tarbell Decl. ¶ 19.

[redacted] Mr. Sayler disagreed with [redacted] the statement in Tarbell's Decl. (Doc. 57, Tarbell Decl. fn 11) regarding the uniqueness of a MAC address, and, therefore, disputed the value of a MAC address for the purpose of identifying a device on a network. Sayler Decl. at ¶ 15. Mr. Sayler knows from his own study, and has published an article explaining that changing a MAC address is a trivial operation on most systems. Id. Mr. Sayler's article appears in an article titled Network Anonymity Through "MAC Swapping". (An article appearing in 2600: The Hacker Quarterly, Volume 28, Issue 3, Autumn 2011. Middle Island, NY.) Id.

Mr. Sayler observed in the trial transcript, that Mr. Ulbricht's laptop was running Ubuntu Linux when the laptop was seized. Sayler Decl., ¶ 16. Knowing that, it would have been a trivial step to change the MAC address of the laptop. Id.

Ulbricht could have substituted other MAC addresses for his own. Id. The MAC address associated with the network adapter on Ulbricht's computer could also have been collected from his computer, and used by other users on networks used by Ulbricht. Id.

These facts - that a MAC address is not a unique identifier and can be easily changed - are widely known. Id.

Mr. Sayler also commented on [redacted]. Mr. Sayler disagrees with that statement, explaining that [redacted] Id., at ¶ 18. Furthermore, Mr. Sayler explains, [redacted]. Id. These facts are also widely known and not new, and contradict [redacted]. Id. According to Sayler, there are numerous ways to change [redacted] Id. Sayler observed that [redacted]

[redacted] Id. Thus, observed Sayler, [redacted] Id.

Mr. Sayler also indicates his disagreement with [redacted] Sayler Decl. at ¶ 19. Mr. Sayler - who is a computer security expert, with a PhD in Computer Science - said that he has seen no data that would support that conclusion. Id. Mr. Sayler also disagrees that [redacted] Id. Mr. Sayler observed that [redacted] and that this, too, is common knowledge in the computer industry. Id.

Mr. Sayler takes exception to [redacted] Sayler Decl. at ¶ 20. Mr. Sayler states that ***the***

[redacted] Mr. Sayler comments that he, himself, often provides [redacted] Id.

Mr. Sayler commented on [redacted] Sayler Decl. at ¶ 21. Mr. Sayler restates that he has seen [redacted] Id. Mr. Sayler also states that it was not surprising that [redacted]

Mr. Sayler noted that [redacted] Sayler Decl. at ¶ 22. Mr. Sayler states that he has not [redacted] seen any basis for the FBI to claim that it had collected data that showed anything communicated to or from Ulbricht's computer. Id.

Mr. Sayler completed his analysis by stating that he had many disagreements with [redacted]

[redacted] and that he has seen no data resulting from PRTT data collection that supports the [redacted] claim to have uniquely identified Ulbricht's computer or any other computer present on the home's network. Sayler Decl. at ¶ 23.

Mr. Sayler stated in his Declaration that he saw no PRTT data that would have allowed the government to identify Ulbricht's computer or any other computer on the home network at the residence where Ulbricht was staying. Id.

ARGUMENT

MR. ULBRICHT IS ENTITLED TO DISCOVER RELEVANT EVIDENCE FOR USE IN HIS MOTION FOR RELIEF PURSUANT TO 28 U.S.C. § 2255, INCLUDING EVIDENCE THAT IS RELEVANT TO HIS CLAIM OF INEFFECTIVE ASSISTANCE OF TRIAL COUNSEL

Mr. Ulbricht intends to submit his motion for relief pursuant to 28 U.S.C. § 2255. In his investigation into grounds for relief, Mr. Ulbricht has determined that he may well have a strong claim of ineffective assistance of trial counsel, for trial counsel's failure to investigate and raise a claim that the search warrant obtained which authorized the seizure and search of Mr. Ulbricht's laptop computer, was obtained based on false and misleading statements provided under oath in the laptop search warrant application.

Evidence obtained from the laptop computer was heavily relied upon by the government in presenting its case against Mr. Ulbricht at his trial. There were government witnesses at trial whose entire testimony was concerned with how Ulbricht's laptop computer was seized and examined, and with what was supposedly found on that computer, and others who made important use of what was supposedly found on Ulbricht's computer. If the evidence obtained from the laptop was obtained in violation of Mr. Ulbricht's Fourth Amendment right to be protected against unreasonable search and seizure, then that evidence should not have been used against him at trial. Had trial counsel discovered the false statements in the laptop search warrant affidavit, and had he moved to suppress the evidence illegally obtained based on that warrant, that evidence would likely have been suppressed. Had the laptop evidence not been used against Ulbricht at trial, the government's case would have been substantially weakened and there is a reasonable probability that the outcome would have been more favorable to Mr. Ulbricht.

Mr. Ulbricht is prepared to show that reasonably competent trial counsel would have investigated and discovered the missing (from discovery) PRTT data, and would have investigated and identified the false statements used to obtain the

laptop search warrant, and would likely have been successful in suppressing the evidence obtained from the laptop, probably leading to a better trial outcome.

These are grounds for vacating or setting aside Mr. Ulbricht's convictions and sentence, and for granting him a new trial. See 28 U.S.C. § 2255(a).

Strategic choices made by trial counsel after thorough investigation of law and facts relevant to the defense are hard to challenge; on the other hand, strategic choices made after less than complete investigation are not reasonable unless counsel made a reasonable decision not to investigate. *Strickland v. Washington*, 466 U.S. 668, 690-691 (1984). The failure of trial counsel to investigate and challenge the veracity of the affiant's statements in the search warrant affidavits, and the failure of trial counsel to notice and object to the fact that the government did not produce in discovery the pen register data its affiant claimed that the FBI had collected, were not the result of reasonable decisions not to investigate, but were the result of neglect by trial counsel. *See Wiggins v. Smith*, 539 U.S. 510, 534 (2003).

Mr. Ulbricht is prepared to show that trial counsel's failure to investigate the veracity of statements in the search warrant applications, and his failure to object to the government's non-production of pen register data that was relied on to obtain the laptop and residence search warrants, resulted in the government being allowed

at trial to use evidence obtained from the laptop and residence search warrants in violation of Ulbricht's Fourth Amendment rights. Had evidence from those illegal searches not been used against Ulbricht, the trial outcome would likely have been more favorable to Ulbricht. Thus, trial counsel's ineffectiveness in failing to adequately investigate and pursue these issues, prejudiced Mr. Ulbricht's defense. For these reasons, Mr. Ulbricht will be able to show that he has met the standards for relief for establishing ineffective assistance of counsel, as set out in *Strickland*. *See Strickland*, 466 U.S. at 687.

The government claimed to have obtained evidence pursuant to pen-trap orders authorizing the FBI to collect pen register and trap and trace data, that enabled them to identify Ulbricht's laptop computer, and to correlate Ulbricht's laptop activity with the internet activity of Dread Pirate Roberts, aka DPR, who supposedly created and ran the Silk Road website, and to "confirm the identify of Ulbricht as DPR." See Doc. 57, Tarbell Decl. (Re Motion to Suppress), ¶¶ 18 -21; Exhibit A, Search and Seizure Warrant, Northern District of California Case No. 3:13-71209 NC.[3]

[3] The 10/1/2013-dated Search and Seizure Warrant and related materials are being filed separately under seal because The Search Warrant Application and Affidavit and the Sealing Order were ordered sealed by the magistrate, and they remain sealed.

Mr. Ulbricht has seen no discovery from the government which supports Mr. Tarbell's claims under oath that the government collected pen register and trap and trace data pursuant to lawful pen-trap orders, and that the data they collected based on that authorization allowed them to identify Ulbricht's computer and track the internet activity of Ulbricht and that computer, and that the data they collected allowed them to "confirm the identify of Ulbricht as DPR." See Doc. 57, Tarbell Decl. ¶¶ 19, 20, 21.

The government has stated that the pen registers were used to determine when Ulbricht was connected to the internet and what IP addresses he was connecting to, and that the data collected consisted of IP address he connected to, along with routing information for his connections, including MAC address for devices connecting to the network. Doc. 56 ¶ 5. No such data has been produced. No data that would have enabled the government to identify Ulbricht's computer, or to track his internet activity, was produced in discovery, as determined by Mr. Sayler's examination of the pen register ("PRTT") data that the government did produce. Given the claims of the government and of Tarbell in his Declaration [redacted] that law enforcement did collect such PRTT data, and the numerous false statements provided in the search warrant affidavits relating to PRTT data collection, the government's failure to produce any

such data (in response to the defense request) should be regarded as an indication that the government wanted to hide the fact that the data never was collected, or that the data was collected by means or methods which violated Mr. Ulbricht's Fourth Amendment rights.

The government obtained five pen-trap orders authorizing the pen register and trap and trace collection of data from Ulbricht's router or from a device associated with a MAC address assumed to be his computer, including 13 MAG 2236, a Sealed Order for the Secret Service, directed to Comcast to provide assistance; 13 MAG 2228, a Sealed Order for the Secret Service, directed to Comcast to provide assistance; 13 MAG 2258 (the 9.19.13 wireless router pen for the FBI); 13 MAG 2274 ((9.20.13.Router Pen for the FBI); and 13 MAG 2275 (9.20.13.MAC Address Pen for the FBI). See Doc. 48, Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress Evidence . . ., at pages 37 -39 (page numbers in original document).

The latter three orders, each of which is directed to the FBI (the three FBI pen-trap orders), were issued in the three sealed magistrate's files (13 MAG 2258, 13 MAG 2274, 13 MAG 2275) which Mr. Ulbricht now wishes to examine.

Mr. Ulbricht argued in his pre-trial motion to suppress (and on direct appeal) that the data collection resulting from the five pen-trap orders should be suppressed

because this data collection required search warrants based on probable cause, not pen-trap orders, and because the orders failed to adhere to statutory limitations. See Doc. 48, Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions to Suppress . . ., at page 37. Mr. Ulbricht's pre-trial Motion to Suppress was hampered by the fact that the government had not disclosed the pen-trap data it had allegedly collected. Because the government failed to disclose all of the pen-trap data, Mr. Ulbricht could only attack the scope of the pen-trap orders, *i.e.*, what they authorized, and he was left to speculate as to what was actually collected.

Mr. Ulbricht now seeks to examine the three sealed magistrate files, to see what data the FBI actually collected, because the government has never produced the data that it claimed [redacted] Mr. Ulbricht has now shown many false and inaccurate statements were provided in the search warrant affidavits regarding [redacted]

The government opposes this motion, *i.e.*, Mr. Ulbricht's request to be allowed access to the three files which should contain the material relevant to the three FBI pen-trap orders and relevant to the government's claims that the PRTT data supported issuance of the laptop search warrant.

Mr. Ulbricht is requesting these magistrates' files be partially unsealed and the contents made available to counsel for both parties and to the defendant, because those files should contain the following material and discoverable information: *"a record which will identify (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device."* 18 U.S.C. § 3123. "The record to be maintained must be provided *ex parte* and under seal to the court which authorized the installation and use of the device within 30 days after termination of the order." *Id*.

Mr. Ulbricht is entitled to examine the contents of the three magistrate files, to see if what the government claimed to have collected (but never produced) was

collected, and to see how any such data was collected. Now that Mr. Ulbricht has shown many false statements in the search warrant affidavit, and now that he has shown the government failed to produce any material and relevant PRTT data in discovery, a decision to withhold from his examination the data in the sealed magistrate's files would be unfair to Mr. Ulbricht and offensive to his due process rights to a fair trial. That information (if it exists) was material to preparation by the defense, was in the possession of the FBI, both before and after the deadline by which the law required it to have been filed with the magistrates, and it should have been disclosed to the defense upon request. See Rule 16(a)(1)(E)(I), Fed.R.Crim.P.

The government told the court that these pen registers were not used to geo-locate Mr. Ulbricht - apparently (since this data was never produced in discovery provided to the defendant) without the government having access to any of the data collected by the FBI pursuant to the three FBI pen-trap orders. Doc. 56 at 5. The three sealed magistrates' files should help answer what pen register data was collected by the FBI, and whether it was collected lawfully, and whether it contained what FBI Special Agent Christopher Tarbell said it contained, under oath, and whether it was used to geo-locate Mr. Ulbricht.

The government has never produced to the defense any of the data collected pursuant to four out of the five pen-trap orders, yet argued before trial against suppression of evidence obtained from the pen registers *on the basis of the government's representation as to what each of the pen registers did and did not collect*. [emphasis added] Doc. 56 at 5. If the government did not have the data, then arguments based on the pretended knowledge of a government attorney were *incautious*, at best, and *deceptive*. If the government had the data but did not produce it upon request, and misrepresented what the data contained in argument to the court, that would be a serious problem. If the government had the data but did not produce it, that alone would constitute a serious discovery violation.

In defending the pen registers against Ulbricht's Fourth Amendment challenge, the government stated that the pen registers were used to establish when Ulbricht logged onto and off of the internet, in support of their argument that the pen register applications to search for information to allow comparison of Ulbricht's online activity with that of DPR, were reasonable and lawful requests seeking relevant information, referencing Doc. 57, Tarbell Decl. ¶ 21. See Doc. 56 at 29-30.

Mr. Ulbricht is entitled to discover whether the undisclosed data supposedly collected and used as the basis for obtaining the laptop and residence search

warrants, was as the government described, or whether the data was collected at all, or whether the data collected was the product of the unreasonable search and seizure of evidence in violation of his Fourth Amendment rights.

The FBI was required by statute to preserve the data they collected, and to file that data and the descriptions as to how and when it was obtained, in the sealed magistrate files identified above, so the data should be there. The sealed files should reveal whether the government and the FBI misrepresented what data was collected from the pen registers.

"Under *Franks v. Delaware*, 438 U.S. 154 (1978), if a search warrant contains a false statement or omission, and the defendant makes a substantial preliminary showing (1) that the false statement or omission was knowingly and intentionally, or with reckless disregard for the truth, included by the government in a search warrant affidavit, (2) that the information was material, and (3) that with the affidavit's false or omitted material aside, the affidavit's remaining content is insufficient to establish probable cause, then the fruits of the search must be suppressed." *United States v. Bianco* , 998 F.2d 1112, 1125 (2d Cir. 1993) (*citing Franks v. Delaware*, 438 U.S. at 155-56, 98 S.Ct. 2674) (emphasis added). "[T]o suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: (1) the claimed inaccuracies or

omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause finding." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013). (internal quotation marks omitted).

The standards set out in *Franks* that will justify exclusion of evidence as a remedy for false statements made to get a warrant do not describe the exclusive remedy for law enforcement actions designed to deceive a court: a "court has 'inherent authority to regulate the administration of criminal justice among the parties before the bar' through its general suppression powers." *United States v. Cortina*, 630 F.2d 1207, 1214 (7th Cir. 1980) *(citing McNabb v. United States*, 318 U.S. 332 (1943)).

Ulbricht has pointed out numerous false statements that were made in the laptop search warrant application. Mr. Sayler has made clear that many of the false statements that he described are widely known to be false, and that other of the false statements are even contradicted by the government's own affiant, in other parts of his affidavit. If the affiant had disclosed that many of his assertions of fact were widely known to be false, or if the magistrate had otherwise learned that important information, the magistrate would not likely have relied on the affidavit. The knowingly or recklessly false statements from the affiant that have been

exposed in Mr. Sayler's declaration involve key factual statements that were obviously made for the purpose of persuading the magistrate that the government had identified Ulbricht as DPR through its PRTT data collection, and that the government had also used that data collection to uniquely identify Ulbricht's computer.

Those false factual statements and fallacious reasoning provided in the search warrant application were used to justify conclusions which Mr. Sayler says are unreasonable and unsupported. Those false statements were key in convincing the magistrate that the government had established probable cause to justify issuance of the laptop [and residence] search warrants.

Those numerous false statements identified by Mr. Sayler cast into doubt the truthfulness of all other factual statements provided by the affiant. If an affiant is willing to make numerous demonstrably false statements in order to obtain a search warrant, it is reasonable to assume that there may well be other, undiscovered false statements in his affidavit. The affiant who intentionally, or knowingly and recklessly, provides numerous false statements to a magistrate under oath, has destroyed his own credibility with regard to any of his statements made under oath. Had the magistrate who issued the laptop and residence search warrants been made aware of the numerous false statements from the affiant that were provided in the

affidavit, he would not likely have found anything the affiant said to be credible and, as a result, would not likely have found that probable cause was established to justify issuance of the laptop (or the residence) search warrant(s).

Mr. Ulbricht has now shown through Mr. Sayler's analysis, that the government did not produce in discovery any relevant and material pen register data, and that the government did not produce any of the key pen register data that Mr. Tarbell [redacted] swore was collected, [redacted]

The three sealed files that Mr. Ulbricht now seeks to examine will reveal whether the government collected the data it claims to have collected in Tarbell's Declaration [redacted] and if that data is not contained in those files, that will be evidence that the government misled the court in opposing the Motion to Suppress and that [redacted]

On the other hand, if the data alleged to have been collected is found in the magistrates' files, along with a record of how the data was collected, as is required by statute, that will support the conclusion that the government violated its discovery obligations by not producing that data in pre-trial discovery. That would suggest that the government deliberately withheld that data, presumably to hide

something. Also, if that data is found in the magistrates' files, along with a record of how it was collected, then the data and the collection methods can be examined to determine whether the data was lawfully collected.

Rule 6 of the § 2255 Rules provides that "a judge may, for good cause shown, authorize a party to conduct discovery under the Federal Rules of Criminal Procedure or Civil Procedure, or in accordance with the practices and principles of law." Rule 6, Discovery, Rules Governing § 2255 Proceedings.

Mr. Ulbricht has established his good cause by showing the importance of the missing data, by showing the likelihood and statutory requirement that it will be located in the three sealed magistrate's files, by showing the many false statements in the search warrant affidavit, and by showing the government's failure to disclose material and relevant data, even though that disclosure was requested.

CONCLUSION

For good cause shown and in the interest of justice, and despite the government's opposition, Mr. Ulbricht respectfully requests an order allowing him to receive and use, as appropriate in his § 2255 proceeding, the content of three sealed magistrate files (13 MAG 2258, 13 MAG 2274, 13 MAG 2275).

Mr. Ulbricht respectfully requests whatever further relief the court finds just and equitable.

Dated: June 11, 2019
Parker, Colorado

/s/ Paul Grant
Paul Grant
Law Office of Paul Grant
19501 E. Mainstreet, Suite 200
Parker, CO 80134
Tel.: 303-909-6133
Email: paul_pglaw@yahoo.com
Counsel for Mr. Ulbricht